

Sophos SafeGuard
Guide de démarrage

Version du produit : 6.1
Date du document : février 2014

Table des matières

1 À propos de ce guide

Ce guide vous indique comment configurer Sophos SafeGuard (SafeGuard Easy 6.1) pour protéger les ordinateurs d'extrémité de votre entreprise contre tout accès non autorisé.

Retrouvez plus d'informations dans le *Manuel d'administration de SafeGuard Easy* et dans le *Manuel d'utilisation de SafeGuard Easy*.

2 À propos de Sophos SafeGuard (SafeGuard Easy)

Sophos SafeGuard (SafeGuard Easy) permet de chiffrer les données de manière transparente : les utilisateurs n'ont pas besoin d'indiquer les données à chiffrer. Le chiffrement et le déchiffrement sont effectués en tâche de fond. Le chiffrement permet d'éviter la consultation ou la modification des données des personnes non autorisées. Le chiffrement Sophos SafeGuard ne peut pas être contourné, même si vous connectez les supports de stockage à un autre système.

Grâce à Sophos SafeGuard, vous pouvez :

- Effectuer une mise en place rapide.
- Protéger la confidentialité des données.
- Chiffrer les données à l'aide d'une technologie certifiée conforme à FIPS 140.

Les ordinateurs d'extrémité protégés par Sophos SafeGuard exécutent l'authentification au démarrage SafeGuard pendant la phase de préinitialisation de l'ordinateur d'extrémité, c'est-à-dire avant le démarrage du système d'exploitation. Une fois que l'utilisateur s'est correctement authentifié dans l'authentification au démarrage SafeGuard, le système d'exploitation démarre et l'utilisateur est connecté à Windows.



L'authentification au démarrage SafeGuard fournit les fonctions conviviales et hautement sécurisées suivantes :

- Protection antialtération pour Sophos SafeGuard Disk Encryption.
- Délais de connexion en cas de saisies erronées.
- Interface utilisateur graphique personnalisable de type Windows.
- Connexion automatique à Windows.
- Prise en charge de plusieurs langues et du format unicode.

Accès administratif facilité

Sophos SafeGuard propose plusieurs fonctions facilitant les opérations informatiques sur les ordinateurs d'extrémité :

- L'authentification au démarrage SafeGuard peut être configurée afin d'être utilisée avec l'éveil par appel réseau, notamment pour faciliter la gestion des correctifs.
- Les comptes de service permettent aux membres de l'équipe informatique de se connecter aux ordinateurs d'extrémité pour réaliser des tâches postérieures à l'installation sans activer l'authentification au démarrage SafeGuard.
- Les utilisateurs de l'authentification au démarrage sont des comptes locaux prédéfinis qui permettent aux utilisateurs (membres de l'équipe informatique, par exemple) de se connecter à des ordinateurs d'extrémité chiffrés pour effectuer des tâches administratives après activation de l'authentification au démarrage SafeGuard.

Options de récupération

Sophos SafeGuard propose plusieurs options de récupération, adaptées à différents scénarios de récupération :

- **Récupération de connexion à l'aide de Local Self Help**

  Local Self Help permet aux utilisateurs ayant oublié leur mot de passe de se connecter à leur ordinateur d'extrémité sans l'aide du support. Les utilisateurs peuvent accéder de nouveau à leur ordinateur d'extrémité même si aucune connexion téléphonique ou réseau n'est disponible (à bord d'un avion, par exemple). Pour se connecter, ils doivent répondre à un certain nombre de questions prédéfinies dans l'authentification au démarrage SafeGuard.

  Local Self Help réduit le nombre d'appels de récupération de connexion, et ainsi les tâches de routine des membres du support en leur permettant de se concentrer sur des demandes plus complexes.

- **Récupération avec Challenge/Réponse**

  Le mécanisme de récupération par Challenge/Réponse implique l'assistance du support. Il vient en aide aux utilisateurs qui ne peuvent pas se connecter à leur ordinateur d'extrémité ou accéder aux données chiffrées. Lors de la procédure Challenge/Réponse, l'utilisateur communique le code de challenge généré sur l'ordinateur d'extrémité au responsable du support qui générera à son tour un code de réponse. Ce code autorisera l'utilisateur à exécuter une action spécifique sur l'ordinateur d'extrémité. Grâce à la procédure de Challenge/Réponse, Sophos SafeGuard propose plusieurs flux de travail pour les scénarios de récupération types nécessitant l'aide du support.

- **Récupération du système**

  Sophos SafeGuard propose divers outils et méthodes destinés à la récupération du système, notamment Windows PE personnalisé par Sophos SafeGuard ou Lenovo Rescue and Recovery. Grâce à ces outils, les problèmes liés au système Windows et aux composants Sophos SafeGuard peuvent être résolus.

La récupération repose sur un fichier de récupération de clé créé pour chaque ordinateur d'extrémité chiffré par Sophos SafeGuard et généralement stocké sur un partage réseau. Cette

clé de récupération garantit que le processus de récupération n'est pas utilisé pour contourner la protection des données. Pour davantage de sécurité, cette clé est également chiffrée. Le partage réseau pour stocker ces fichiers, ainsi que les droits d'accès requis pour ce partage, sont créés automatiquement au cours de la configuration initiale.

2.1 À propos de Sophos SafeGuard (SafeGuard Easy) 6.1

Sophos SafeGuard assure une protection puissante des données à travers le chiffrement et une authentification supplémentaire à la connexion.

Cette version de Sophos SafeGuard (SafeGuard Easy) prend en charge Windows 7 et Windows 8 sur des ordinateurs d'extrémité dotés de BIOS ou d'UEFI.

- Pour les plates-formes BIOS, vous pouvez choisir entre le chiffrement intégral du disque Sophos SafeGuard et le chiffrement BitLocker administré par Sophos SafeGuard. La version BIOS est livrée avec le mécanisme de récupération BitLocker original.

  Remarque : si l'authentification au démarrage SafeGuard ou le chiffrement intégral du disque SafeGuard sont mentionnés dans le présent manuel, il font uniquement référence aux ordinateurs d'extrémité Windows 7 avec BIOS.

- Pour les plates-formes UEFI, veuillez utiliser BitLocker géré par Sophos SafeGuard (SafeGuard Easy) pour le chiffrement du disque. Pour ces ordinateurs d'extrémité, Sophos SafeGuard offre des fonctionnalités améliorées de Challenge/Réponse. Retrouvez plus de renseignements sur les versions UEFI prises en charge et sur les limites de la prise en charge du Challenge/Réponse SafeGuard BitLocker dans les Notes de publication disponibles sur http://downloads.sophos.com/readmes/readsgeasy_61_fra.html.

Remarque : la mention UEFI apparaît de manière explicite à chaque fois qu'elle doit être utilisée.

Le tableau ci-dessous indique quels composants sont disponibles.

	Chiffrement intégral du disque SafeGuard avec authentification au démarrage SafeGuard	Authentification de préinitialisation BitLocker gérée par SafeGuard	Récupération C/R SafeGuard pour l'authentification de préinitialisation BitLocker
Windows 7 BIOS	**OUI**	**OUI**	
Windows 7 UEFI		**OUI**	**OUI**
Windows 8 UEFI		**OUI**	**OUI**
Windows 8 BIOS		**OUI**	
Windows 8.1 UEFI		**OUI**	**OUI**
Windows 8.1 BIOS		**OUI**	

Remarque : la **Récupération C/R SafeGuard pour l'authentification de préinitialisation BitLocker** est uniquement disponible sur les systèmes 64 bits.

Le **Chiffrement intégral du disque SafeGuard avec authentification au démarrage SafeGuard** est le module Sophos permettant de chiffrer les volumes sur les ordinateurs d'extrémité. Il est livré avec l'authentification de préinitialisation Sophos nommée authentification au démarrage SafeGuard qui prend en charge les options de connexion par cartes à puce, par empreinte digitale et qui offre un mécanisme Challenge/Réponse pour la récupération.

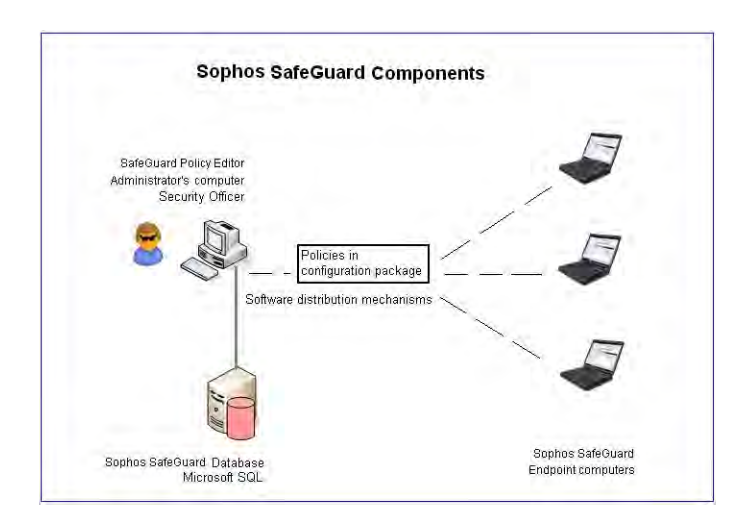
L'**Authentification de préinitialisation BitLocker gérée par SafeGuard** est le composant qui active et gère le moteur de chiffrement BitLocker et l'authentification de préinitialisation BitLocker.

Elle est disponible sur les plates-formes BIOS et UEFI :

- La version UEFI propose également un mécanisme Challenge/Réponse SafeGuard pour la récupération de BitLocker lorsque l'utilisateur oublie son code PIN. La version UEFI peut être utilisée si la plate-forme répond à certaines conditions préalables requises. Par exemple, la version UEFI doit être 2.3.1. Retrouvez plus de renseignements dans les Notes de publication.
- La version BIOS ne propose pas toutes les fonctions de récupération offertes par le mécanisme Challenge / Réponse SafeGuard. Elle sert d'option de secours lorsque les conditions requises à l'utilisation de la version UEFI ne sont pas remplies. Le programme d'installation Sophos vérifie si les conditions requises sont remplies et en cas contraire, il installe automatiquement la version BitLocker sans Challenge/Réponse.

Pour protéger les informations sur les ordinateurs d'extrémité, Sophos SafeGuard (SafeGuard Easy) utilise une stratégie de chiffrement.

L'administration s'effectue via SafeGuard Policy Editor utilisé pour créer et gérer les stratégies de sécurité et pour proposer des fonctions de récupération. Les stratégies sont déployées sur les ordinateurs d'extrémité via des packages de configuration. Côté utilisateur, les fonctions de sécurité principales sont le chiffrement des données et la protection contre l'accès non autorisé. Sophos SafeGuard peut être intégré de façon transparente à l'environnement normal de l'utilisateur, et son utilisation est facile et intuitive. L'authentification au démarrage SafeGuard, le système d'authentification de Sophos SafeGuard, fournit une protection efficace des accès et propose une assistance conviviale lors de la récupération des codes d'accès.



Composants Sophos SafeGuard

Sophos SafeGuard est constitué des composants suivants :

Composant	Description
SafeGuard Policy Editor	L'outil de gestion Sophos SafeGuard permet de créer des stratégies de chiffrement et d'authentification. SafeGuard Policy Editor crée une stratégie par défaut lors de la toute première configuration. SafeGuard Policy Editor contient par ailleurs des fonctions de récupération pour permettre à l'utilisateur de retrouver l'accès à son ordinateur, lorsqu'il a oublié son mot de passe, par exemple.
Base de données Sophos SafeGuard	La base de données Sophos SafeGuard contient tous les paramètres de stratégie des ordinateurs d'extrémité.
Logiciel Sophos SafeGuard sur les ordinateurs d'extrémité	Logiciel de chiffrement sur les ordinateurs d'extrémité

Noms de produit

Les noms de produit suivants sont utilisés dans cette aide :

Nom de produit	Description
Sophos SafeGuard Easy (SGE)	Logiciel de chiffrement autonome Sophos SafeGuard. À partir des versions 5.x, SafeGuard Policy Editor est utilisé pour les tâches de configuration des stratégies et de support technique.

Nom de produit	Description
Sophos SafeGuard Disk Encryption (SDE) jusqu'à 5.60	Logiciel de chiffrement autonome Sophos SafeGuard disponible avec l'offre groupée Endpoint Security and Data Protection (ESDP) jusqu'à la version 10.
Sophos Disk Encryption 5.61	Chiffrement intégral du disque administré via la version 5.1 et versions supérieures de la Sophos Enterprise Console.
SafeGuard Enterprise	Suite de chiffrement SafeGuard étendue et modulaire avec administration centralisée à base de rôles qui empêche la lecture ou le changement des données par des personnes non autorisées sur les ordinateurs d'extrémité.
Sophos Enterprise Console	Console Sophos qui administre et met à jour le logiciel de sécurité Sophos. Avec la version 5.1, elle administre également le chiffrement sur les ordinateurs d'extrémité (Sophos Disk Encryption 5.61).

3 Mise à niveau à partir d'anciennes versions

Les ordinateurs d'extrémité déjà chiffrés avec la version 5.60.x ou supérieure de SafeGuard Easy/Sophos SafeGuard Disk Encryption peuvent être mis à niveau vers SafeGuard Easy 6.1.

Un fichier de licence valide est nécessaire afin de vous permettre d'effectuer l'importation dans SafeGuard Policy Editor. Votre partenaire commercial devrait vous avoir envoyé ce fichier.

Retrouvez plus d'informations aux sections *À propos de la mise à niveau* et *À propos de la migration* du *Manuel d'administration de SafeGuard Easy*.

4 Que dois-je installer ?

Installez les composants suivants :

- **SafeGuard Policy Editor**. La console d'administration de Sophos SafeGuard. Elle vous permet de gérer le logiciel de chiffrement sur les ordinateurs d'extrémité et d'effectuer les tâches de récupération.

  Microsoft SQL Server 2012 SP1 Express Edition est utilisé pour stocker les paramètres de stratégie de Sophos SafeGuard. Il est installé automatiquement au cours de la configuration de SafeGuard Policy Editor en cas d'absence d'une instance du serveur Microsoft SQL.

  Remarque : installez d'abord SafeGuard Policy Editor sur un serveur Windows. Ensuite, vous pourrez l'installer sur plusieurs ordinateurs d'administrateurs connectés à la base de données Sophos SafeGuard centrale du serveur.

- **Logiciel de chiffrement Sophos SafeGuard.** Il procède au chiffrement des données sur les ordinateurs d'extrémité et assure leur protection contre tout accès non autorisé.

  Remarque : nous déconseillons l'installation du logiciel de chiffrement sur les ordinateurs sur lesquels SafeGuard Policy Editor est installé.

5 Quelles sont les étapes principales ?

Effectuez les étapes suivantes :

- Installez SafeGuard Policy Editor.
- Procédez à la première configuration en créant une stratégie par défaut et en définissant les conditions requises les plus importantes pour effectuer les tâches du support.
- Copiez la stratégie par défaut pour pouvoir la modifier.
- Attribuez l'accès administrateur aux ordinateurs d'extrémité suite à l'installation.
- Publiez la stratégie modifiée dans un package de configuration.
- Installez le logiciel de chiffrement et le package de configuration sur les ordinateurs d'extrémité.

6 Installation de SafeGuard Policy Editor

Avant de commencer :

- Assurez-vous que .NET Framework 4 est installé sur l'ordinateur sur lequel vous voulez installer SafeGuard Policy Editor. Il est livré avec le produit.
- Si vous voulez installer Microsoft SQL Server 2012 SP1 Express Edition automatiquement lors de l'installation de SafeGuard Policy Editor, assurez-vous que Microsoft Windows Installer 4.5 est installé.
- Consultez la configuration système requise dans les Notes de publication.
- Assurez-vous de disposer des droits d'administrateur Windows.

Pour installer SafeGuard Policy Editor :

1. Ouvrez une session sur votre ordinateur en tant qu'administrateur.
2. À l'aide de l'adresse Web et des codes d'accès de téléchargement fournis par votre administrateur système, allez sur le site Web Sophos et téléchargez le programme d'installation et la documentation.
3. Placez-les à un emplacement auquel vous pouvez accéder pour effectuer l'installation.
4. Dans le dossier d'installation du produit, cliquez deux fois sur le package SGNPolicyEditor.msi de SafeGuard Policy Editor. Un assistant vous guide tout au long des étapes nécessaires.
5. Acceptez les valeurs par défaut dans les boîtes de dialogue suivantes.

   Si vous êtes invité à installer Microsoft SQL Server 2012 SP1 Express Edition, cliquez sur **Oui**. Dans ce cas, vos codes d'accès Windows sont utilisés pour le compte utilisateur SQL.
6. Cliquez sur **Terminer** pour terminer l'installation.

SafeGuard Policy Editor est installé. Vous pouvez à présent effectuer la première configuration dans SafeGuard Policy Editor.

7 Exécution de la configuration initiale

Assurez-vous de disposer des droits d'administrateur Windows.

1. Démarrez SafeGuard Policy Editor dans le menu **Démarrer**. L'assistant de configuration démarre et vous guide tout au long des étapes nécessaires.
2. Sur la page **Bienvenue**, cliquez sur **Suivant**.
3. Sur la page **Base de données**, cliquez sur **Suivant**. La base de données SQL pour l'archivage des paramètres et des stratégies SafeGuard est créée.
4. Sur la page **Responsable de la sécurité**, saisissez et confirmez un mot de passe pour accéder au SafeGuard Policy Editor. Cliquez sur **Suivant**. Le certificat du responsable de la sécurité est créé.

   Conservez le mot de passe en lieu sûr. Si vous le perdez, vous ne pourrez plus accéder au SafeGuard Policy Editor. Le personnel du support informatique doit disposer d'un accès au compte afin de pouvoir exécuter les tâches de récupération.

   Le nom du responsable de la sécurité s'affiche.
5. Sur la page **Entreprise**, cliquez sur **Suivant**. Le certificat d'entreprise est utilisé pour sécuriser les paramètres de stratégie de la base de données et des ordinateurs d'extrémité.
6. Sur la page **Sauvegarde des certificats d'entreprise et du responsable de la sécurité**, définissez un emplacement de stockage sûr pour les sauvegardes de certificats. Puis cliquez sur **Suivant**.

   Si vous sauvegardez les certificats dans l'emplacement de stockage par défaut dès maintenant, assurez-vous de les exporter dans un emplacement sûr et accessible en cas de besoin de récupération. Vous pouvez par exemple utiliser une clé USB à mémoire flash immédiatement après la configuration initiale. Vous aurez besoin de ces certificats pour restaurer une installation défectueuse ou une base de données corrompue de SafeGuard Policy Editor.
7. Sur la page **Clés de récupération**, cliquez sur **Suivant**. Un partage réseau avec les droits suffisants pour le personnel du support informatique est créé. Ce partage sert à récupérer les fichiers de clés de récupération à partir des ordinateurs d'extrémité requis pour effectuer la récupération.
8. Sur la page **Licence**, cliquez sur **[...]** pour naviguer jusqu'au fichier de licence valide et exécuter SafeGuard Policy Editor en environnement de production. Votre partenaire commercial devrait vous avoir envoyé le fichier de licence. Sélectionnez le fichier et cliquez sur **Ouvrir**. Cliquez sur **Suivant**.
9. Cliquez sur **Terminer**.

La première configuration est terminée.

- Une stratégie par défaut a été créée afin de pouvoir appliquer la stratégie de sécurité globale de l'entreprise sur tous les ordinateurs d'extrémité.
  - L'authentification au démarrage SafeGuard est activée.
  - Le chiffrement intégral de disque SafeGuard pour tous les disques durs internes est activé.
  - Le chiffrement à base de fichiers pour les données des supports amovibles est activé.

- L'utilisateur peut récupérer un mot de passe oublié à l'aide de Local Self Help en répondant aux questions prédéfinies.
- Le support peut récupérer les mots de passe à l'aide de la procédure Challenge/Réponse.

- Les conditions requises au support pour pouvoir effectuer les tâches de récupération ont été définies.
- Un fichier de licence valide est importé pour pouvoir exécuter Sophos SafeGuard en environnement de production.

SafeGuard Policy Editor démarre dès que l'assistant de configuration se ferme.

8 Copie de la stratégie par défaut pour modification

1. Dans la zone de navigation de SafeGuard Policy Editor, cliquez sur **Stratégies**.
2. Dans la fenêtre de navigation **Stratégies**, sous **Groupes de stratégies**, cliquez avec le bouton droit de la souris sur **Stratégie par défaut** et cliquez sur **Sauvegarder la stratégie**.
3. Saisissez un nom de fichier et un emplacement de stockage pour la copie (XML) et cliquez sur **Enregistrer**.
4. Dans la fenêtre de navigation, cliquez avec le bouton droit de la souris sur **Groupes de stratégie**, puis cliquez sur **Restaurer une stratégie**.
5. Sélectionnez la nouvelle copie de la stratégie (XML) et cliquez sur **Ouvrir**.

Une copie de la stratégie par défaut incluant tous les éléments de la stratégie individuelle est importée dans SafeGuard Policy Editor.

Personnalisez ensuite la copie de la stratégie par défaut pour configurer une liste de comptes de service pour un accès administratif aux ordinateurs d'extrémité suite à l'installation. Ainsi, vous êtes sûr que le personnel de maintenance peut accéder et préconfigurer les ordinateurs d'extrémité après l'installation du logiciel de chiffrement sans avoir à être enregistré.

9 Accès des administrateurs aux ordinateurs d'extrémités

Le personnel de maintenance pourrait avoir besoin d'accéder et de préconfigurer l'ordinateur d'extrémité une fois que le logiciel de chiffrement a été installé, par exemple, via un déploiement central. Toutefois, le premier utilisateur qui se connecte à l'ordinateur suite à l'installation du logiciel de chiffrement active l'authentification au démarrage SafeGuard puis il est ajouté comme utilisateur Sophos SafeGuard aux ordinateurs d'extrémité. Pour éviter cela, vous pouvez les inclure dans une liste de comptes de service. Les membres du personnel de maintenance inclus dans cette liste peuvent alors se connecter au système d'exploitation de l'ordinateur d'extrémité suite à l'installation et effectuer les tâches nécessaires sans activer l'authentification au démarrage SafeGuard et sans être ajouté comme utilisateur Sophos SafeGuard.

Pour configurer une liste de comptes de service :

1. Dans la zone de navigation de SafeGuard Policy Editor, cliquez sur **Stratégies**.
2. Dans la fenêtre de navigation **Stratégies**, cliquez avec le bouton droit de la souris sur **Listes de comptes de service**, cliquez sur **Nouveau** et sur **Liste de comptes de service**.
3. Saisissez un nom pour la liste et cliquez sur **OK**.
4. Dans la fenêtre de navigation **Listes de comptes de service**, sélectionnez la nouvelle liste.
5. Cliquez avec le bouton droit de la souris dans la zone d'action, à droite, et sélectionnez **Ajouter** dans le menu contextuel. Une nouvelle ligne utilisateur est ajoutée.
6. Saisissez le **Nom d'utilisateur** et le **Nom du domaine** dans les colonnes respectives, puis appuyez sur Entrée. Répétez cette étape pour ajouter d'autres utilisateurs. Retrouvez plus d'informations à la section *Informations supplémentaires pour la saisie de nom d'utilisateur et de domaine* du *Manuel d'administration de SafeGuard Easy*.
7. Cliquez sur l'icône **Enregistrer** de la barre d'outils pour enregistrer vos modifications dans la base de données.

   La liste de comptes de service est désormais enregistrée. Dans les étapes suivantes, vous pouvez l'affecter à une stratégie.

8. Dans la fenêtre de navigation, sous **Éléments de stratégie**, sélectionnez l'élément de stratégie **Authentification** qui a été copié.
9. Sous **Options de connexion**, sélectionnez la nouvelle liste créée dans **Liste de comptes de service**.
10. Cliquez sur l'icône **Enregistrer** de la barre d'outils pour enregistrer vos modifications.

La liste de comptes de service est configurée. L'élément de stratégie **Authentification** et le groupe de stratégies dont il fait partie sont respectivement mis à jour. Publiez ensuite la stratégie modifiée dans un package de configuration.

Remarque : vous pouvez modifier d'autres paramètres de stratégie selon vos besoins. Par exemple, pour personnaliser l'authentification au démarrage SafeGuard, configurer le chiffrement ou activer l'éveil par appel réseau. Retrouvez plus d'informations à la section *Éveil par appel réseau sécurisé (WOL)* du *Manuel d'administration de SafeGuard Easy*.

10 Publication de la stratégie dans un package de configuration

Pour mettre les stratégies à disposition sur les ordinateurs d'extrémité, publiez-les d'abord dans un package de configuration.

1. Démarrez SafeGuard Policy Editor, sélectionnez **Outils** et cliquez sur **Outil de package de configuration**.
2. Cliquez sur **Ajouter un package de configuration**.
3. Donnez un nom au package de configuration.
4. Sélectionnez un **Groupe de stratégies** modifié à l'étape précédente et qui sera appliqué aux ordinateurs d'extrémité.
5. Indiquez un emplacement de stockage pour le package de configuration.
6. Cliquez sur **Créer un package de configuration**.
7. Cliquez sur **Fermer**.

La stratégie est publiée dans un package de configuration (MSI) à l'emplacement spécifié. Installez ensuite le logiciel de chiffrement Sophos SafeGuard et le package de configuration sur les ordinateurs d'extrémité.

11 Installation du logiciel de chiffrement et du package de configuration sur les ordinateurs d'extrémité

1. Préparez l'ordinateur d'extrémité au chiffrement
2. Pour vous familiariser avec Sophos SafeGuard, commencez par installer le logiciel de chiffrement sur un ordinateur réservé à l'évaluation. Utilisez un ordinateur différent de celui sur lequel SafeGuard Policy Editor est installé.
3. Connectez-vous une première fois.
4. Utilisez vos propres outils pour créer et distribuer les packages d'installation et de configuration afin de configurer de manière centralisée le logiciel de chiffrement sur les ordinateurs d'extrémité.

11.1 Préparation des ordinateurs d'extrémité au chiffrement.

- Assurez-vous qu'un compte utilisateur est configuré et activé. L'utilisateur doit avoir un mot de passe.
- Assurez-vous de disposer des droits d'administrateur Windows.
- Créez une sauvegarde complète des données.
- Les lecteurs à chiffrer doivent être complètement formatés et disposer d'une lettre de lecteur.
- Sophos fournit une liste des configurations matérielles afin de réduire le risque de conflits entre l'authentification au démarrage SafeGuard et le matériel de votre ordinateur d'extrémité. La liste est fournie avec le package d'installation du logiciel de chiffrement.

  Nous vous conseillons d'installer une version mise à jour de ce fichier de configuration avant de procéder au déploiement de Sophos SafeGuard. Ce fichier bénéficie d'une mise à jour mensuelle et peut être téléchargé depuis l'emplacement suivant : http://www.sophos.com/fr-fr/support/knowledgebase/65700.aspx.
- Recherchez les erreurs sur le(s) disque(s) dur(s) à l'aide de la commande suivante :

  `chkdsk %lecteur% /F /V /X`

  Dans certains cas, vous pouvez être invité à redémarrer votre ordinateur d'extrémité et à exécuter de nouveau la commande **`chkdsk`**. Retrouvez plus d'informations sur : http://www.sophos.com/fr-fr/support/knowledgebase/107081.aspx .

  Vous pouvez vérifier les résultats (fichier journal) dans l'Observateur d'événements Windows :

  Windows 7 : Sélectionnez **Journaux Windows** , **Application**, **Wininit**.
- Utilisez l'outil de défragmentation de Windows appelé **`defrag`** pour localiser et consolider les éléments fragmentés, notamment les fichiers d'initialisation, les fichiers de données et les dossiers sur les volumes locaux.

  `defrag %drive%`

Retrouvez plus d'informations sur :
http://www.sophos.com/fr-fr/support/knowledgebase/109226.aspx.

- Désinstallez les gestionnaires d'initialisation tiers, tels que PROnetworks Boot Pro et Boot-US.
- Nous vous conseillons de nettoyer le MBR (master boot record). Pour installer Sophos SafeGuard, votre MBR doit être unique et sain. Suite à l'utilisation d'outils d'image/de clone sur l'ordinateur d'extrémité, il se peut que le MBR ne soit plus sain.

  Démarrez l'ordinateur d'extrémité à partir d'un DVD Windows et utilisez la commande **`FIXMBR`** dans la Console de récupération Windows. Retrouvez plus d'informations sur :
  http://www.sophos.com/fr-fr/support/knowledgebase/108088.aspx.
- Si la partition d'initialisation de l'ordinateur d'extrémité a été convertie du format FAT au format NTFS et si l'ordinateur n'a pas été redémarré depuis, redémarrez l'ordinateur une fois. Sinon, il se peut que l'installation ne se soit pas terminée avec succès.

11.2 Installation d'une version d'évaluation

Procédez à l'installation d'une version d'évaluation du logiciel de chiffrement sur un ordinateur différent de celui sur lequel SafeGuard Policy Editor est installé.

Conditions préalables :

Les ordinateurs d'extrémité doivent avoir été préparés pour le chiffrement. Retrouvez plus d'informations à la section Préparation des ordinateurs d'extrémité au chiffrement à la page 19.

1. Ouvrez une session sur l'ordinateur d'extrémité en tant qu'administrateur.
2. Installez le package de préinstallation **`SGxClientPreinstall.msi`** le plus récent, qui fournira à l'ordinateur d'extrémité la configuration requise pour une installation réussie du logiciel de chiffrement courant.
3. Cliquez deux fois sur le package du logiciel de chiffrement **SGNClient.msi** ou sur sa variante en 64 bits si nécessaire. Un assistant vous guide tout au long des étapes nécessaires.
4. Acceptez les valeurs par défaut dans les boîtes de dialogue suivantes.
5. Si vous y êtes invité, sélectionnez le type d'installation **Complète**.

   Le chiffrement intégral du disque SafeGuard et le chiffrement à base de fichiers de SafeGuard sont installés. Retrouvez plus d'informations sur les packages et les fonctions de chiffrement disponibles à la section *Installation* du *Manuel d'administration de SafeGuard Easy*.
6. Acceptez les valeurs par défaut dans toutes les boîtes de dialogue suivantes pour terminer l'assistant d'installation.
7. Accédez à l'emplacement d'enregistrement du package de configuration (MSI).
8. Installez ce package de configuration sur l'ordinateur d'extrémité. Assurez-vous que tous les packages d'installation obsolètes ont été supprimés de l'ordinateur d'extrémité.

Sophos SafeGuard est installé et configuré conformément aux stratégies déjà créées sur l'ordinateur d'extrémité. Connectez-vous ensuite à l'ordinateur après l'installation, soit pour

effectuer les tâches postérieures à l'installation (à l'aide d'un compte de service) soit en tant qu'utilisateur normal.

Une configuration supplémentaire peut être requise pour garantir que l'authentification au démarrage SafeGuard fonctionne correctement sur chaque plate-forme matérielle. La majorité des conflits matériels peuvent être résolus à l'aide de la fonction **Raccourcis clavier** intégrée à l'authentification au démarrage SafeGuard. Retrouvez plus d'informations à la section *Raccourcis clavier pris en charge dans l'authentification au démarrage* du *Manuel d'administration de SafeGuard Easy*. Consultez aussi :

http://www.sophos.com/fr-fr/support/knowledgebase/107781.aspx et

http://www.sophos.com/fr-fr/support/knowledgebase/107785.aspx.

11.3 Première connexion à l'aide d'un compte de service

Connectez-vous à l'aide d'un compte de service si vous souhaitez effectuer les tâches postérieures à l'installation sur l'ordinateur d'extrémité.

1. Redémarrez l'ordinateur d'extrémité suite à l'installation. La boîte de dialogue de connexion Windows apparaît.

   Appuyez tout d'abord sur les touches CTRL+ALT+SUPPR pour vous connecter. L'administrateur peut désactiver ce paramètre dans la console MMC de l'éditeur d'objet de stratégie de groupe sous **Paramètres Windows** > **Paramètres de sécurité** > **Stratégies locales** > **Désactiver les options de sécurité** (pour la connexion interactive, il n'est pas nécessaire d'appuyer sur CTRL+ ALT+ SUPPR).

2. Connectez-vous à Windows à l'aide de votre compte de service : saisissez le domaine et les codes d'accès définis auparavant dans la liste des comptes de service dans SafeGuard Policy Editor.

Vous êtes connecté à Windows en tant qu'utilisateur invité. L'authentification au démarrage SafeGuard n'est pas activée et vous n'êtes pas enregistré sur l'ordinateur d'extrémité. Vous pouvez procéder aux tâches postérieures à l'installation nécessaires.

11.4 Première connexion en tant qu'utilisateur

1. Redémarrez l'ordinateur. La connexion automatique à Sophos SafeGuard apparaît suivi de la connexion à Windows.

   Appuyez tout d'abord sur les touches CTRL+ALT+SUPPR pour démarrer la connexion automatique et vous connecter. L'administrateur peut désactiver ce paramètre dans la console MMC de l'éditeur d'objet de stratégie de groupe sous **Paramètres Windows** > **Paramètres de sécurité** > **Stratégies locales** > **Désactiver les options de sécurité** (pour la connexion interactive, il n'est pas nécessaire d'appuyer sur CTRL+ ALT+ SUPPR).

2. Saisissez votre nom d'utilisateur et votre mot de passe Windows.
3. Redémarrez l'ordinateur d'extrémité une deuxième fois. L'authentification au démarrage SafeGuard est activée.

4. Saisissez votre nom d'utilisateur et votre mot de passe Windows. Vous êtes automatiquement connecté à Windows.

   L'authentification au démarrage SafeGuard est maintenant activée. Vous êtes enregistré en tant qu'utilisateur Sophos SafeGuard. Une infobulle de confirmation apparaît. À votre prochaine ouverture de session, vous devrez uniquement saisir vos codes d'accès Windows à l'authentification au démarrage SafeGuard.

Le chiffrement initial démarre automatiquement. Vous pouvez continuer à travailler et il n'est pas nécessaire de redémarrer l'ordinateur d'extrémité à la fin du chiffrement. N'arrêtez pas l'ordinateur ou ne le mettez pas en hibernation avant la fin du chiffrement initial. Tous les processus de chiffrement et de déchiffrement sont exécutés de manière transparente sans nécessiter aucune intervention de l'utilisateur. Retrouvez plus d'informations dans le *Manuel d'utilisation de SafeGuard Easy*.

11.5 Installation du logiciel de chiffrement et des packages de configuration à l'aide d'un script

1. Préparez l'installation sur les ordinateurs d'extrémité. Retrouvez plus d'informations à la section Préparation des ordinateurs d'extrémité au chiffrement à la page 19.
2. Ouvrez une session sur l'ordinateur administrateur en tant qu'administrateur.
3. Créez un dossier appelé **`Logiciels`** à utiliser pour centraliser le stockage de toutes les applications.

4. Utilisez un outil de déploiement de logiciels comme Microsoft System Center Configuration Manager, IBM Tivoli ou Enteo Netinstall pour exécuter l'installation centrale sur les ordinateurs d'extrémité. Les éléments suivants doivent être inclus dans l'ordre mentionné :

   Remarque : lors de l'exécution de l'installation via Active Directory, utilisez un objet de stratégie de groupe (GPO, group policy object) distinct pour chaque package et triez-les dans l'ordre mentionné ci-dessous pour garantir une installation réussie.

   Si la langue de l'ordinateur d'extrémité n'est pas définie sur vos paramètres régionaux, procédez aux modifications supplémentaires suivantes : dans l'Éditeur de stratégies de groupe, sélectionnez l'objet de groupe respectif et **Configuration de l'ordinateur** > **Paramètres logiciels**> **Avancés**. Dans la boîte de dialogue **Options de déploiement avancées**, sélectionnez **Ignorer la langue lors du déploiement de ce package** et cliquez sur **OK**.

Package	Description
Package de préinstallation **`SGxClientPreinstall.msi`**	Pour une installation réussie du logiciel de chiffrement actuel, le package obligatoire fournit les configurations requises aux ordinateurs d'extrémité. **Remarque :** Si ce package n'est pas installé, l'installation du logiciel de chiffrement échoue.
Package du logiciel de chiffrement	En fonction de votre licence et de votre système d'exploitation, différents packages d'installation sont disponibles. Tous les packages disponibles (<*Client*>.MSI) se trouvent dans votre produit. **Remarque :** Retrouvez une liste de tous les packages disponibles à la section *Installation* du *Manuel d'administration de SafeGuard Easy*.
Package de configuration pour les ordinateurs d'extrémité	Utilisez le package de configuration créé auparavant dans SafeGuard Policy Editor. Assurez-vous d'avoir d'abord supprimer tous les packages de configuration obsolètes.
Script avec les commandes de l'installation préconfigurée	Nous vous conseillons d'utiliser l'outil de ligne de commande de Windows Installer **`msiexec`** pour créer le script. Retrouvez plus d'informations à la section *Commande pour l'installation centralisée* du *Manuel d'administration de SafeGuard Easy* ou consultez : http://msdn.microsoft.com/fr-fr/library/aa367988(VS.85).aspx

5. Pour créer le script, ouvrez une invite de commande et saisissez les commandes de script. Retrouvez plus d'informations à la section Exemple de commande de script à la page 24.
6. Distribuez la préinstallation, le package du logiciel de chiffrement, le package de configuration et le script sur les ordinateurs d'extrémité à l'aide des mécanismes de distribution de logiciels de l'entreprise.

   Les packages sont exécutés sur les ordinateurs d'extrémité.

7. Après l'installation, assurez-vous que les ordinateurs d'extrémité ont été redémarrés deux fois pour activer l'authentification au démarrage SafeGuard. Ils doivent être redémarrés une troisième fois pour effectuer une sauvegarde des données de noyau à chaque initialisation Windows.

   Assurez-vous que les ordinateurs d'extrémité ne sont pas suspendus ou en veille prolongée avant le troisième redémarrage pour exécuter avec succès la sauvegarde du noyau.

Sophos SafeGuard est installé et configuré en fonction de la configuration des stratégies précédemment créées sur les ordinateurs d'extrémité. Un fichier de récupération de clé est créé pour chaque ordinateur d'extrémité à l'emplacement défini lors de la première configuration de SafeGuard Policy Editor.

Remarque : une configuration supplémentaire peut être requise pour garantir que l'authentification au démarrage SafeGuard fonctionne correctement sur chaque plate-forme matérielle. La plupart des conflits matériels peuvent être résolus à l'aide de la fonction **Raccourcis clavier** intégrée à l'authentification au démarrage SafeGuard. Retrouvez plus d'informations à la section *Raccourcis clavier pris en charge dans l'authentification au démarrage* du *Manuel d'administration de SafeGuard Easy.* Consultez aussi :

http://www.sophos.com/fr-fr/support/knowledgebase/107781.aspx et

http://www.sophos.com/fr-fr/support/knowledgebase/107785.aspx.

11.6 Exemple de commande de script

```
msiexec /i F:\Software\Sophos\SafeGuard\SGxClientPreinstall.msi
 /qn
```

```
msiexec /i F:\Software\Sophos\SafeGuard\SGNClient.msi /qn /L*VX
 G:\Temp\Sophos\SafeGuard\%nomordinateur%_SGNClient_inst.log
Installdir=C:\Program Files\Sophos\Sophos SafeGuard
```

```
msiexec /i F:\Software\Sophos\SafeGuard\SGNClientConfig.msi
/qn
```

Cette commande a l'effet suivant :

- ```
  msiexec /i
  F:\Software\Sophos\SafeGuard\SGxClientPreinstall.msi
  ```

  Installe le package de préinstallation de Sophos SafeGuard à partir de l'emplacement de stockage défini dans le répertoire d'installation par défaut : **`C:\Program Files\Sophos\Sophos SafeGuard`**. Les ordinateurs d'extrémité sont fournis avec la configuration requise pour garantir la réussite de l'installation du logiciel de chiffrement.

- ```
  msiexec /i F:\Software\Sophos\SafeGuard\SGNClient.msi
  ```

  ```
  Installdir=C:\Program Files\Sophos\Sophos SafeGuard
  ```

  Installe le logiciel de chiffrement, ici le chiffrement intégral du disque SafeGuard avec l'authentification au démarrage SafeGuard à partir de l'emplacement de stockage défini dans le répertoire d'installation par défaut : **`C:\Program Files\Sophos\Sophos SafeGuard`**.

- ```
  msiexec /i F:\Software\Sophos\SafeGuard\SGNClientConfig.msi
  ```

  Installe le package de configuration à partir de l'emplacement de stockage spécifié dans le répertoire d'installation par défaut.

- ```
  /L*VX
  G:\Temp\Sophos\SafeGuard\%nomordinateur%__SGNClient_inst.log
  ```

  Enregistre tous les avertissements et messages d'erreur dans le fichier journal spécifié stocké sur le réseau et crée un fichier journal pouvant être analysé automatiquement à l'aide de l'outil de Windows Installer **`wilogutl.exe`**.

- ```
  /qn
  ```

  Procède à l'installation sans intervention de l'utilisateur et n'affiche pas d'interface utilisateur.
  ```

12 Récupération d'un mot de passe oublié

Si l'utilisateur a oublié son mot de passe, il existe deux manières de le récupérer :

- L'utilisateur peut le récupérer via Local Self Help. Nous vous conseillons d'utiliser cette méthode.
- Le support peut le récupérer via une procédure Challenge/Réponse.

12.1 Récupération d'un mot de passe oublié via Local Self Help

1. L'utilisateur saisit son nom d'utilisateur dans l'authentification au démarrage SafeGuard, sur l'ordinateur d'extrémité.

   Le bouton **Récupération** devient actif.

2. L'utilisateur clique sur **Récupération**.
   - Si seule la méthode Local Self Help est activée sur l'ordinateur d'extrémité pour la récupération de la connexion, elle démarre automatiquement.
   - Si les méthodes Local Self Help et challenge/réponse sont disponibles pour la récupération de la connexion, l'utilisateur clique sur **Local Self Help**.

3. Dans les cinq boîtes de dialogue suivantes, l'utilisateur répond à un nombre défini de questions sélectionnées aléatoirement parmi les questions stockées sur l'ordinateur d'extrémité. Après avoir répondu à la dernière, l'utilisateur confirme ses réponses en cliquant sur **OK**.
4. Dans la boîte de dialogue suivante, l'utilisateur peut voir le mot de passe en appuyant sur la touche Entrée, sur la barre d'espace ou en cliquant sur la case bleue.

   Le mot de passe s'affiche pendant 5 secondes maximum. Ensuite, le processus de démarrage continue automatiquement. L'utilisateur peut immédiatement masquer le mot de passe en appuyant de nouveau sur la touche Entrée, sur la barre d'espace ou en cliquant de nouveau sur la case bleue.

5. Après avoir lu le mot de passe, l'utilisateur clique sur **OK**.

L'utilisateur est connecté à l'authentification au démarrage SafeGuard et à Windows et pourra utiliser le mot de passe pour se connecter ultérieurement.

12.2 Récupération d'un mot de passe oublié via Challenge/Réponse

Conditions préalables :

Le fichier de récupération de clé créé de chaque ordinateur d'extrémité lors de l'installation du logiciel de chiffrement Sophos SafeGuard doit être accessible au support et son nom doit être connu. La méthode Challenge/Réponse doit être activée via une stratégie sur l'ordinateur d'extrémité.

Remarque :

Nous vous conseillons d'utiliser en priorité Local Self Help pour récupérer un mot de passe oublié. Local Self Help permet à l'utilisateur d'afficher le mot de passe actuel et de continuer à l'utiliser. Ceci lui évite d'avoir à réinitialiser le mot de passe ou de demander de l'aide au support technique.

1. L'utilisateur saisit son nom d'utilisateur dans l'authentification au démarrage SafeGuard, sur l'ordinateur d'extrémité. Le bouton **Récupération** devient actif.
2. L'utilisateur clique sur **Récupération**.

   - Si seule la méthode Challenge/Réponse est activée pour la récupération de la connexion, elle démarre automatiquement.
   - Si les méthodes Challenge/Réponse et Local Self Help sont disponibles pour la récupération de la connexion, l'utilisateur clique sur **Challenge/Réponse**.

   Une boîte de dialogue indiquant le nom du fichier de récupération de clé requis s'affiche.
3. L'utilisateur clique sur **Suivant**. Un code de challenge généré de manière aléatoire s'affiche.
4. L'utilisateur contacte le support. Il lui fournit le nom du fichier de récupération de clé requis ainsi que le code de challenge.
5. Dans SafeGuard Policy Editor, le support lance l'**Assistant de récupération**.
6. Le support sélectionne le type de récupération **Client Sophos SafeGuard** , confirme la clé et le code de challenge, puis sélectionne l'action de récupération souhaitée **Initialiser le client SGN sans connexion utilisateur**.

   Un code de réponse sous la forme d'une chaîne de caractères ASCII est généré puis affiché.
7. Le support transmet le code de réponse à l'utilisateur, par exemple par téléphone ou SMS.
8. Sur l'ordinateur d'extrémité, dans l'assistant Challenge/Réponse, l'utilisateur clique sur **Suivant** pour saisir le code de réponse fourni. L'ordinateur d'extrémité peut démarrer à partir de l'authentification au démarrage SafeGuard.
9. Dans la boîte de dialogue d'ouverture de session Windows, l'utilisateur ne connaît pas le mot de passe et doit par conséquent le modifier au niveau Windows. Cela nécessite d'autres actions de récupération sortant du périmètre de Sophos SafeGuard, via des moyens Windows standard. Nous vous conseillons d'utiliser les méthodes de réinitialisation de mot de passe Windows ci-dessous :

   - À l'aide d'un compte de service ou administrateur disponible sur l'ordinateur d'extrémité avec les droits Windows requis.
   - À l'aide d'un disque de réinitialisation de mot de passe Windows sur l'ordinateur d'extrémité.
10. L'utilisateur saisit le nouveau mot de passe Windows fourni par le support. L'utilisateur modifie ensuite ce mot de passe immédiatement en choisissant une valeur connue de lui seul.

    Un nouveau certificat utilisateur à utiliser dans Sophos SafeGuard sera créé automatiquement en fonction du nouveau choix de mot de passe Windows. Cela permet à l'utilisateur de se reconnecter à l'ordinateur ainsi qu'à l'authentification au démarrage SafeGuard à l'aide du nouveau mot de passe.

L'utilisateur peut ouvrir une session sur l'ordinateur, se connecter de nouveau à l'authentification au démarrage SafeGuard avec son nouveau mot de passe et pourra utiliser celui-ci pour ses prochaines ouvertures de session.

13 Aide sur les tâches générales

Cette section vous indique où trouver les informations relatives à la réalisation des tâches générales. Retrouvez plus d'informations dans le *Manuel d'administration*, dans le *Manuel d'utilisation* ou dans le *Guide des outils de SafeGuard Easy*.

Tâche	Manuel/Aide
Configuration des instances supplémentaires de SafeGuard Policy Editor	Manuel d'administration : configuration des instances supplémentaires de SafeGuard Policy Editor
Garantie du bon fonctionnement de l'authentification au démarrage SafeGuard	Manuel d'administration/Manuel d'utilisation : raccourcis clavier pris en charge dans l'authentification au démarrage SafeGuard
Affichage des informations spécifiques à Sophos SafeGuard sur l'ordinateur d'extrémité	Manuel d'utilisation : icône de la barre d'état système et infobulle
Création et regroupement des stratégies	Manuel d'administration : utilisation de stratégies
Exportation des certificats	Manuel d'administration : exportation des certificats d'entreprise et du responsable de la sécurité.
Création de l'accès administratif aux ordinateurs d'extrémité (comptes d'accès à l'authentification au démarrage).	Manuel d'administration : accès administratifs aux ordinateurs d'extrémité
Récupération de l'accès aux données chiffrées	Récupération de l'accès aux données chiffrées avec Challenge/Réponse
Récupération d'un Master Boot Record corrompu	Guides des outils : restauration d'un MBR corrompu
Migration de SGE/SDE 5.60.x ou supérieure vers SafeGuard Easy 6.1	Guide de mise à niveau : à propos de la mise à niveau

14 Support technique

Vous bénéficiez du support technique des produits Sophos de l'une des manières suivantes :

- Rendez-vous sur le forum de la communauté SophosTalk en anglais sur http://community.sophos.com/ et recherchez d'autres utilisateurs rencontrant le même problème que le vôtre.
- Rendez-vous sur la base de connaissances du support de Sophos sur http://www.sophos.com/fr-fr/support.aspx/.
- Téléchargez la documentation des produits sur http://www.sophos.com/fr-fr/support/documentation/.
- Envoyez un e-mail à support@sophos.fr, y compris le(s) numéro(s) de version du logiciel Sophos, le(s) système(s) d'exploitation et le(s) niveau(x) de correctif ainsi que le texte de tous les messages d'erreur.

15 Mentions légales